

REMARKS

Claims 5-13, 15-25, 27-37 and 39-40 were presented for examination and are still pending in this application. In an Official Action dated October 31, 2003, claims 5-13, 15-25, 27-37 and 39-40 were rejected. Applicants thank Examiner for examination of the claims. Applicants now request reconsideration in light of the below remarks and allowance of claims 5-13, 15-25, 27-37 and 39-40.

In paragraph 8 of the Office Action, Examiner rejects claim 5 under § 102(e) over U.S. Patent No. 6,408,391 issued to Huff et al. ("Huff"). The rejection is respectfully traversed. Presently prented claim 5 recites a system for protecting a network, comprising:

a vulnerability detection system (VDS) for gathering information about the network to determine vulnerabilities of a plurality of hosts on the network; and

an intrusion detection system (IDS) for examining network traffic responsive to the vulnerabilities of a host from the plurality of hosts as determined by the VDS to detect traffic indicative of malicious activity.

Thus, claim 5 provides a VDS that discovers vulnerabilities of a system and an IDS that leverages this information to examine network traffic directed at a host for attacks on these vulnerabilities. Advantageously, information sharing between the VDS and IDS provides efficient and targeted intrusion detection.

By contrast, Huff discloses *only* an IDS that is aware of *only* actual intrusions. (See Huff 1:5-10). More specifically, Huff discloses agents configured around nodes of a network. (Huff 8:39-52). These agents "monitor[] the computers on the network for misuse and intrusion." (Huff 3:20-21; also 10:54-11:6). In response to an actual misuse or intrusion, Huff discloses a security computer taking "defensive and/or offensive measures to suppress or counterattack the intruder or misuser by automatically sending defensive or offensive agents to the computer on which a suspected or actual intrusion or misuse occurred." (Huff 3:23-27).

However, Huff fails to disclose or suggest the invention as described in claim 5 either alone or in combination with the other cited references. First, Huff fails to disclose a VDS. Applicants have examined the entire reference and respectfully submit that there

is no determination of vulnerabilities of hosts on the network. Note that Huff's detection of *actual misuses and intrusions* are known in the art to be of a different nature than the *vulnerabilities* of claim 5. While the former relates to an actual attack in progress, the latter is merely a potential point of attack. Second, Huff fails to disclose an IDS that responds to host vulnerabilities since the agents in Huff are not aware of potential attacks, only actual attacks. Third, it follows that Huff fails to distinguish the vulnerabilities of one host from other hosts while examining traffic. Therefore, Applicants respectfully submit that claim 5 is patentable over Huff either alone or in combination with the other cited references.

Since claims 6-13 and 15-16 depend upon independent claim 5, and recite additional patentable features, these claims are patentably distinguishable for at least the same reasons as claim 6.

Independent claims 17 and 29 are of similar scope to claim 5, and thus are patentable for at least the same reasons. Furthermore, since claims 18-25 and 27-28 depend upon claim 17, and 30-37 and 39-40 depend upon claim 29, and recite additional patentable features, these claims are patentably distinguishable for at least the same reasons as claims 17 and 29.

Additionally, Applicant respectfully disagrees with Examiner's assertion in paragraph 10 concerning claims 15-16, 27-28 and 39-40. More specifically, Examiner takes Official Notice that the VDS updating determined vulnerabilities, and the IDS detecting traffic indicative of updated vulnerabilities would be obvious to one of ordinary skill in the art. The IDS would not detect traffic indicative of updated vulnerabilities because, as discussed above, the IDS is not even aware of vulnerabilities unless configured according to the present invention. If Examiner wishes to maintain this assertion, Applicants respectfully request supporting evidence. (See MPEP 2144.03(C)).

CONCLUSION

In sum, Applicant respectfully submits that claims 5-13, 15-25, 27-37 and 39-40, as presented herein, are patentably distinguishable over Huff and/or the other cited references. Therefore, Applicant requests reconsideration and allowance of these claims.

In addition, Applicant respectfully invites Examiner to contact Applicant's representative at the number provided below if Examiner believes it will help expedite furtherance of this application.

RESPECTFULLY SUBMITTED,

Date: December 31, 2003

By: Dorian Cartwright

Dorian Cartwright, Attorney of Record
Registration No. 53,853
FENWICK & WEST LLP
Silicon Valley Center
801 California Street
Mountain View, CA 94041
Phone: (650) 335-7247
Fax: (650) 938-5200